Symantec™ Mobile Management 7.2 SP3 Release Notes

Symantec™ Mobile Management 7.2 SP3 Release Notes

This document includes the following topics:

- About Mobile Management
- What's new in Mobile Management 7.2 SP3
- Upgrading Symantec Mobile Management
- Fixed issues in Symantec™ Mobile Management 7.2 SP3
- Known issues for Symantec™ Mobile Management 7.2 SP3

About Mobile Management

Symantec Mobile Management lets you manage, secure, and troubleshoot the mobile devices in your organization. Using Mobile Management, you can automate IT tasks and control your IT environment more effectively. By becoming more effective, you can reduce the effort and costs of managing, securing, and troubleshooting mobile devices. Mobile Management works with the Symantec Management Platform to simplify the management of and communication with the devices in your environment.

What's new in Mobile Management 7.2 SP3

In the 7.2 SP3 release of Symantec Mobile Management, the following new features are introduced:

- Support for iOS 7 (not including iOS 7 MDM features)
  The following articles also address Symantec Mobile Management compatibility with iOS 7:
  - Unable to Enroll or Manage iOS 7 Device
    http://www.symantec.com/docs/TECH209766
  - Point fix: iOS 7 Device Support for SMM
    http://www.symantec.com/docs/TECH209914
  - How to use the MDM Agent Builder Application
    http://www.symantec.com/docs/TECH210048
- Samsung SAFE features and mobile device support
- Supports Android 4.3
- SCEP server payload settings now have new SCEP unique challenge settings. SCEP unique challenge can be defined to provide certificates to mobile devices without using a shared challenge password. A unique challenge password is used only one time to request one certificate.
- iOS NitroDesk TouchDown support. TouchDown is now supported on iOS mobile devices.
- Windows Phone 8 is supported for app and content delivery.
- Installs on Symantec Management Platform 7.5

Several changes have been made to the Mobile Management UI to enhance usability. Key UI changes include:

- Location of the TouchDown payload settings in the Configuration Editor. The **TouchDown Account**, **TouchDown Policy**, and **TouchDown User Settings** are now contained in the TouchDown Configuration section.
- **Samsung SAFE Configuration** payload settings have been added to the Configuration Editor. These payload settings include **Restrictions**, **Credentials**, **VPN**, **Device Options**, **Wi-Fi**, **EAS**, **Email**, and **Kiosk Mode**.

Upgrading Symantec Mobile Management

Use the following procedure to update to latest version of Symantec Mobile Management:

Prerequisites for upgrading to Symantec Mobile Management 7.2 SP3

- Upgrading to version 7.2 SP3 is only supported from version 7.2 SP2. If your current installation is an earlier version that 7.2 SP2, you must first upgrade to 7.2 SP 2. Be aware of the following warnings:

Warning: The update to Symantec Mobile Management 7.2 SP1 or later from 7.2 or earlier can result in the loss of WiFi connectivity for managed iOS devices. The managed devices that have a WiFi profile are affected. Read the knowledge base article TECH194739 *Loss of Device Wi-Fi Communication After Upgrade of SMM to 7.2 SP1* for more information about this issue.

Some installations may also lose authentication services. For more information and instructions to correct the problem, see the Symantec knowledge base article TECH197019, Authentication stops working after upgrading to Symantec Mobile Management 7.2 SP1.

Warning: If using F5 rules and your environment has custom iRule requirements, manually remove the iRule cache file (C:\ProgramData\Symantec\MobileManagement\eas_rule.txt). Replace this cache file with the new version by running the NS.Quarter-Hour{5834ae07-1160-4037-8a25-67aebf6a254e} scheduled task after upgrading. Replacing the cache file allows the iRule definition version to update to the new version. The iRule definition version is not automatically changed during an upgrade to the latest Symantec Mobile Management version. TouchDown configuration fails as a result.

To upgrade Symantec Mobile Management

1. Log in as the service account (application identity) and make sure that it has local admin rights.
2. You upgrade Mobile Management through the Symantec Installation Manager. Go to **Start > All Programs > Symantec > Symantec Installation Manager**. Right-click the Symantec Installation Manager and select **Run as administrator**.
3. On the **Installed Products** page, click **Upgrade installed products.**.
4. Select *Symantec Mobile Management* with the correct version number of the upgrade, and click **Next**.
5. On the **Optional Installations** page, click **Next**
6. Accept the EULA and click **Next**.
7. On the **Contact Information** page, click **Next**.

8 Verify the installation details and click **Next**.

9 On the **Installation Complete** page, click **Finish**.

Note: After an upgrade, Exchange ActiveSync configuration is lost. If using EAS, you must rerun the eas.bat batch file after the upgrade to restore the EAS server information. Then, you can re-configure EAS functionality. For more information about the eas.batch file, see the Symantec knowledge base article TECH201454, Configuration of EAS Integration Using the EAS ConfigTool.

During an upgrade, the database is locked, and communication between the Symantec Management Platform Notification Server and the site server is stopped. The site server still attempts to communicate with the Notification Server computer. This situation can cause errors and issues. After you install Mobile Management 7.2 SP3, you must upgrade Mobile Management servers manually in the Symantec Management Console to complete the upgrade. Use this procedure to upgrade Symantec Mobile Management servers:

Upgrading the Mobile Management Server manually

1 In the Symantec Management Console, click **Home > Mobile Management > Settings > Mobile Management Server Settings**

2 In the right pane, highlight the site server and then on the toolbar, click **Upgrade**.

3 Repeat Step 2 for each server.

4 Click **Save changes**

For more information about upgrading the products that use the Symantec Management Platform, see Symantec Knowledge-base article HOWTO 44338, Installing an update or an additional product.

Fixed issues in Symantec™ Mobile Management 7.2 SP3

The following issues from previous releases are fixed in this release.

- Device can't install certificate when 'Require SSL' in IIS SSL settings is enabled.
- In the Mobile Inventory, all Android devices indicate that TouchDown is installed even when the TouchDown client is not installed on the device.
- Mismatch in the "Camera Enabled" setting between the Configuration Editor Device Options payload and the Applied Settings page.

- In-house applications with the same name are incorrectly managed in the Mobile Library.
- The SMM servers pass N/A AD/LDAP test passwords in cleartext between the Notification Server and site servers.
- The 'ForcedSMIMEPinTimeout' TouchDown policy setting is not supported.
- The 'DisablePrinting' TouchDown policy setting is not supported.
- iOS 7 does not obtain a valid SMTP sender address from Exchange Server using generic EAS configuration profile.
- Device "LastUpdateDateTime" and "LastConnected" times are not correct.
- Network or IIS service failure between MMS and NS cause device inventory to stop processing and fail to recover after services have resumed.
- APNS feedback for certain devices directs them to be no longer managed.
- VPN profile asks for password twice when trying to enable VPN.

Known issues for Symantec™ Mobile Management 7.2 SP3

The following are known issues for this release.

Table 1-1

Issue	Cause	Workaround
Upgrade of in-house agents from 4857 to 5025 causes agent reset.	Server forces reset when it cannot match the records on an existing device.	Re-enroll the agent.
Mobile Library installed applications are un-installed. While inventory shows them removed, the buttons of the agent never change back to "install".	N/A	Re-enroll the agent.

Table 1-1 *(continued)*

Issue	Cause	Workaround
When a generic EAS profile is sent to a Samsung SAFE-enabled device, the password field of the login widget shows four asterisks. If you elect to show the password, the word "Null" is displayed.	As-designed	Replace the four characters with the password you use to access your email
A file in the CAB Trackerlog.exe was changed from previous versions because the “standing” health metric for this file (a filehash metric) was incorrect for this embedded version of the this file in the current CAB file.	N/A	Perform a “regenerate” action in the Altiris Console for the **Mobile Management Agent for WinCE5 ARMV4i -> Health**
Certificates or apps are not displayed in Device Inventory for WP 7 and 8 Windows Phone devices.	N/A	Not currently supported
Samsung SAFE: if the device is in Kiosk mode and you update policies, the device will go through a "remove" and "created" process each time the policy is sent.	Per Samsung design	See knowledge base article: http://www.symantec.com/docs/TECH210525
Error "settings failed to save" on iOS Enrollment page after you delete used certificate from Configuration Editor.	The certificate is used as part of the iOS Enrollment Settings.	Do not delete the certificate.
Touchdown unconfigured policies reset configured policies on Android devices.	N/A	Some policy settings require that you enter values. For these values to take effect, you must also enable the setting by placing a checkmark in the setting's check box.

Table 1-1 *(continued)*

Issue	Cause	Workaround
Mobile devices receiving EAS policy do not appear on EAS Policy Assignment page.	By design	See knowledge base article: http://www.symantec.com/docs/TECH210364
Mobile Management kiosk-mode policy allows out-of-band user interaction.	N/A	See knowledge base article: http://www.symantec.com/docs/TECH210327
Settings screen closes unexpectedly or does not appear at all on Samsung SAFE devices enrolled with Mobile Management.	Third-party functionality	Refer to Samsung documentation.
Enrollment fails when you attempt to enroll Windows Mobile devices.	The Mobile Management web configuration file requires that the DNS suffix is a fully qualified domain name (FQDN).	See knowledge base article: http://www.symantec.com/docs/TECH210329